REMARKS

Claims 35 and 36 are pending in this application.

Claims 35 and 36 were rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 6,134,328 in view of Fischer (U.S. Patent No. 4,868,877). A Terminal Disclaimer is being filed concurrently herewith.

Claims 35 and 36 were rejected under 35 U.S.C. §103(a) as being unpatentable over Fischer (U.S. Patent No. 4,868,877) in view of Kuzma (U.S. Patent No. 5,771,289). Reconsideration is respectfully requested.

The present invention is directed to a secure user certification system for electronic commerce that provides an accounting system for services provided. In electronic commerce, various parties conduct activities without face to face contact. As such, it is desirable for each party to any transaction to be able to determine and verify the authenticity of the other party to the transaction, as well as ensure sufficient security for any commerce conducted electronically. Such security services could include, for example, message integrity, message authentication, message confidentiality, and message non-repudiation. In an electronic commerce environment these security services are achieved by cryptographic techniques such as digital signature, hash codes, encryption algorithms, and the like. To effectively implement the above, a party to an electronic commerce transaction requires access to a secure cryptographic device capable of securely implementing these cryptographic techniques. According to the present invention, a certificate meter provides certificate management services including use of cryptographically secured certificates. Payment for the processing and issuing, by the certificate authority, of the electronic certificates, also referred to as electronic postmarks, can be made using funds stored in the meter. Thus, the present invention provides a party to an electronic commerce transaction access to a secure cryptographic device, i.e., a certificate meter, associated with a certificate authority, while providing the certificate authority with a convenient payment system to allow the certificate authority to get paid for processing and issuing of the electronic certificates (postmarks).

In view of the above, claim 35 is directed to a method for validating a signed digital message the comprises "providing a register having funds stored therein; receiving a signed digital message from a sender; determining if sufficient funds are present in the register for validating the message; deducting funds from the register for validating the message; and validating the signed digital message using a public key of the sender."

Fischer is directed to a public key cryptographic system with enhanced digital signature certification that authenticates the identity of the public key holder. Specifically, in Fischer, a trusted authority creates a digital message which contains the claimant's public key and the name of the claimant and a representative of the authority signs the digital message with the authority's own digital signature. This digital message, often referred to as a certificate, is sent along with the use of the claimant's own digital signature. Any recipient of the claimant's message can trust the signature, provided that the recipient recognizes the authority's public key. (Col. 3, lines 21-34).

Thus, while Fischer discloses the use of certificates for providing security functions, as noted by the Office Action, there is no disclosure, teaching or suggestion in Fischer of providing payment to the certificate authority for processing, i.e., validating, the signed digital mesage.

To overcome the above deficiency, the Office Action relies on the reference to Kuzma. Kuzma is directed to a method and apparatus for transmitting electronic data using electronic credits to pay for the transmission. In Kuzma, a transmission service provides communications links between a sender and an addressee. The sender uses electronic stamps, previously purchased from the transmission service, to pay for the transmission of the message and the use of the communications links, After preparing an electronic message for sending and selecting an addressee, the file size is examined, for example in bytes, of the data being transmitted and an electronic stamp is attached to the data transmission as payment for the transmission and/or use of the communications channel. The electronic stamp is a data packet that when processed by the carrier or at the addressee location appears as a stamp-like graphic marking on the transmitted document. Substantially concurrently with application of the electronic stamp to the electronic data, a counter or database containing the data corresponding to the sender's amount of electronic stamps is debited in an amount equal to the value of the affixed electronic stamp to reflect the use of the electronic stamp to pay for the electronic transmission of the data or message. (Col. 2, line 53 to Col. 3, line 9). To prevent fraud and theft of services of the carrier, the stamp presented as payment for a transmission can be authenticated by hiding an authenticating mark in the stamp graphics or by including an authentication data code. (Col. 3, lines 17-44). There is no disclosure, teaching or suggestion in Kuzma of signed digital messages or validating a signed digital message.

The Office Action contends that it would have been obvious to combine these references to arrive at the present invention. Applicants respectfully disagree. As noted above, Kuzma is directed to a method and system for paying for an electronic transmission. If one were motivated to combine the teachings of Fischer and Kuzma, it would simply teach a method and system to <u>pay a transmission service for the electronic transmission of the digital message created and signed by the trusted authority</u>. There is no disclosure, teaching or suggestion in the cited references, either alone or in combination, of a method for validating a signed digital message that includes "providing a register having funds stored therein; receiving a signed digital message from a sender; determining if sufficient funds are present in the register for validating the message; deducting funds from the register for validating the message; and validating the signed digital message using a public key of the sender" as recited in claim 35.

Without using the present claims as a road map, it would not have been obvious to make the multiple, selective modifications needed to arrive at the claimed invention from these references. The rejection uses impermissible hindsight to reconstruct the present invention from these references. See Ex parte Clapp, 227 U.S.P.Q. 972,973 (Bd. App. 1985) (requiring "convincing line of reasoning" to support and obviousness determination).

The fact that the present invention was made by the Applicants does not make the present invention obvious; that suggestion or teaching must come from the prior art. See C.R. Bard, Inc. v. M3 Systems, Inc., 157 F.3d 1340, 1352 (Fed. Cir. 1998). See, e.g., Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 1051-1052 (Fed. Cir. 1988) (it is impermissible to reconstruct the claimed invention from selected pieces of prior art absent some suggestion, teaching, or motivation in the prior art to do so). "Determination of obviousness can not be based on the hindsight combination of components selectively culled from the prior art to fit the parameters of the patented invention. There must be a teaching or suggestion within the prior art, or within the general knowledge of a person of ordinary skill in the field of the invention, to look to particular sources of information, to select particular elements, and to combine them in a way they were combined by the inventor." ATD Corp. v. Lydall, Inc., 159 F.3d 534, 545 (Fed. Cir. 1998) (emphasis added). No such suggestion or motivation has been provided by the Office Action to arrive at the present invention from these references.

For at least the above reasons, it is respectfully submitted that claim 35 is allowable over the prior art of record. Claim 36, dependent upon claim 35, is allowable along with claim 35 and on its own merits.

In view of the foregoing remarks, it is respectfully submitted that the claims of this case are in a condition for allowance and favorable action thereon is requested.

Respectfully submitted,

Brian A. Lemm
Reg. No. 43,748
Attorney for Applicants
Telephone (203) 924-3836

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000